ՏԵԽՆԻԿԱԿԱՆ ԲՆՈՒԹԱԳԻՐ - ԳՆՄԱՆ ԺԱՄԱՆԱԿԱՑՈՒՅՑ\*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Ծառայության | | | | | |
| հրավերով նախատեսված չափաբաժնի համարը | գնումների պլանով նախատեսված միջանցիկ ծածկագիրը` ըստ ԳՄԱ դասակարգման (CPV) | տեխնիկական բնութագիրը | չափ-ման միա-վորը | մատուցման | |
| հասցեն | Ժամկետը\* |
| 1 | 64211340/6 | **էլեկտրոնային տեղեկատվական ծառայություններ՝ այդ թվում**  հաջորդ սերնդի բարձր արդյունավետությամբ միջցանցային էկրան (Firewall), UTM/UTP ծառայություն՝  - Անտիվիրուս  - IPS/IDS  - Անտիսպամ  - Վեբ և վիդեո ֆիլտրում  - Application Control  - Botnet IP/Դոմեյն  - Cloud sandbox  Պետք է ապահովել, որ սարքը հնարավորություն ունենա միավորվելու բարձր հասանելիության կլաստերի մեջ: Կլաստերի պետք է աշխատի ակտիվ-ակտիվ կամ ակտիվ-պասիվ կամ կլաստերային ռեժիմում:  Կլաստերի բոլոր սարքերը պետք է ունենան կառավարման և մոնիտորինգի կենտրոնացված ինտերֆեյս, առանց լրացուցիչ ծրագրային կամ ապարատային բաղադրիչների։  Հրապատը պետք է ապահովվի հետևյալ հնարավորությունները՝   * Firewall, IPsec, IPS, Antivirus, Antispam, content filtering, appliance software, intrusion detection, adware & malware removal tools, advanced threat detection, VPN ֆունկցիաները, տրաֆիկի կառավարում (traffic shaping), WLAN controller կետերի հասանելիության ֆունկցիա, Real-time SSL inspection (including TLS 1.3), դինամիկ IPv4, IPv6 երթուղավորում, WAN-միացումների օպտիմալացում,WEB և Video ֆիլտրացում, Հավելվածների վերահսկողությունը (Application Control), ինտեգրում Active Directory հետ, ունենա վեբ-պրոքսի ֆունկցիա   Հրապատը պետք է ունենա առնվազն՝   * 18 հատ ապարատային արագացմամբ GE RJ45 port, որը ներառում է՝ 1 հատ GE RJ45 MGMT ինտերֆեյս կառավարման համար, 1 հատ RJ45 HA ինտերֆեյս և 16 հատ GE RJ45 switch port * 8 հատ ապարատային արագացմամբ GE SFP ինտերֆեյս * 4 հատ ապարատային արագացմամբ 10GE SFP+ (FortiLink աջակցությամբ) ինտերֆեյս * 1 հատ RJ45 Console Port * 1 հատ USB ինտերֆեյսներ * Բոլոր անհրաժեշտ բաղադրիչների առկայություն 19″ սերվերային պահարանում ներկառուցման համար, իսկ բարձրությունը պետք է լինի ոչ ավել, քան 1 RU * 2 հոսանքի սնուցման աղբյուր (Redundant Power Supplies AC PSU 80Plus Compliant for 1+1 Redundancy) * Առանձնացված Security Processing Unit (SPU)   Հրապատը պետք է ապահովվի հետևյալ Արտադրողականությունը՝   * Firewall ցանցային էկրանի թողունակությունը առնվազն 39 Գբիտ/վ. * Threat Protection թողունակությունը՝ 2․8 Գբիտ/վ * Մեկ վայրկյանում առնվազն 42 միլիոն փաթեթի թողունակություն * IPSec VPN (512 byte) թողունակությունը առնվազն 35 Գբիտ/վ * SSL-VPN թողունակությունը առնվազն 1․5 Գբիտ/վ * IPS թողունակությունը առնվազն 5․3 Գբիտ/վ * Միաժամանակյա սեսիաներ (TCP) առնվազն 3 միլիոն * Նոր սեսսիաները առնվազն 140,000 սեսիա մեկ վայրկյանում * Միաժամանակյա IPsec VPN հաճախորդ-շլյուզ միացումների քանակը առնվազն 16,000 * Միաժամանակյա IPsec VPN շլյուզ-շլյուզ միացումների թիվը առնվազն 2000 * Firewall-ի քաղաքականությունների թիվը առնվազն 10000 * Օգտագործողի անսահմանափակ արտոնագիր * Security Processing Unit (SPU) պետք է ապահովի 520 Գբիտ/վ թողունակություն   «Ցանցային որդերի» հակավիրուսային պաշտպանության / հայտնաբերման եւ ոչնչացման մոդուլը պետք է ունենա հետեւյալ հնարավորությունները՝   * Ստուգել HTTP, SMTP, POP3, IMAP, FTP պրոտոկոլները եւ IM-ծառայությունները, ստուգել գաղտնագրված VPN թունելները * Հակավիրուսային բազաների թարմացումների ավտոմատ «օպերատիվ առաքում» * Վարակված հաղորդագրությունները կարանտինի մեջ տեղադրելու հնարավորություն * Արգելափակում՝ կախված ֆայլի ծավալից և տեսակից   Ցանցային գործառույթները՝   * SD-WAN հնարավորություն, LoadBalance, Failover, բազմակի WAN ինտերֆեյսների օգտագործման հնարավորությամբ * PPPoE, DHCP, DNS սերվեր աշխատելու հնարավորություն * Քաղաքականությունների վրա հիմնված երթուղայնացում, դինամիկ երթուղայնացում (RIP v1 և v2, OSPF, BGP, Multicast), գոտիներ բաժանման հնարավոթյուն, գոտիների միջեւ երթուղայնացում, վիրտուալ ցանցերի(VLAN) միջև երթուղայնացում * Հնարավորություն ձևավորել տրամաբանական SD-WAN ինտերֆեյս՝ միավորելով ֆիզիկական եւ տրամաբանական ինտերֆեյսները տարատեսակ միացումներով (MPLS, լայնաշերտ ինտերնետ, LTE և այլն) * SD-WAN ուղիների որակի գնահատում՝ փաթեթներ կամ հարցումներ ուղարկելով ցանցի կոնկրետ հանգույցներին * Ուղիների բնութագրերի վերահսկողություն իրական ժամանակի ռեժիմում (packet loss փաթեթի կորուստ, Jitter ցնցում, latency ուշացում) և դրանց գրաֆիկական ցուցադրում * Հաղորդակցման ուղիների ընտրման բազմակողմանի ռազմավարությունների սահմանում հավելվածների տրաֆիկի երթուղայնացման համար՝ ելնելով SLA համապատասխանության չափանիշներից, կապի ուղիների բնութագրերի լավագույն արժեքներից և այլն: * Հավելվածների տրաֆիկի երթուղայնացման և սերվիսների կանոնների սահմանում SD-WAN ալիքների միջոցով, հաշվի առնելով ռազմավարությունները և SLA-ն * Կապի ուղիների բեռնվածության ավտոմատ հավասարակշռում, փոխանջատում և պահեստավորում օգտագործվող հավելվածների և ծառայությունների համար, ցանցային կապերի(loss կորուստ, Jitter ցնցում, latency ուշացում) բնութագրերի փոփոխության ժամանակ, ռեալ ժամանակում * Դինամիկ կերպով ուղղում փաթեթի կորուստները կամ սխալ փաթեթների վերականգնում, որոնք առաջանում են վատ WAN-ուղիների պայմանների պատճառով, երբ աշխատում են VPN-ի միջոցով (ForwardError Correction) * Մեկ սեսիայի փաթեթների հավասարակշռումը երկու IPSec VPN թունելների միջոցով, որոնք հիմնված են "per packet" հավասարակշռու-թյան վրա   Վարչարարություն կառավարում՝   * Դերերի վրա հիմնված կառավարում, ադմինիստրատորների եւ օգտագործողների մի քանի մակարդակներ, թարմացումներ և փոփոխություններ TFTP պրոտոկոլի և web ինտերֆեյսի միջոցով, համակարգային ծրագրային ապահովման մեջ նախկին վիճակի վերադարձ   Օգտագործողների նույնականացում՝   * Ներկառուցված օգտատերերի տվյալների բազա * Արտաքին RADIUS/LDAP տվյալների բազայի միացման հնարավորություն * IP/MAC հասցեով կցելու հնարավորություն * Երկգործոնային նույնականացմում (two-factor authentication) * PKI և սերտիֆիկատներ՝ X.509, SCEP support, Certificate Signing Request (CSR) ստեղծում, ավտոմատ սերտիֆիկատների թարմացում ժամկետի ավարտից առաջ, OCSP աջակցություն   Firewall-ը պետք է ունենա հետեւյալ առանձնահատկությունները՝   * NAT, PAT, «թափանցիկ» (կամուրջ) * Երթուղայնացման ռեժիմ (RIP v1 եւ v2, OSPF, BGP,Multicast) * NAT հիմնված քաղաքականությունների վրա * Վիրտուալ դոմեններ (NAT/Transparent Mode), VLAN Tagging (802.1Q), SIP/H.323 NAT Traversal, WINS * Օգտագործողների խմբերի վրա հիմնված նույնականացում, * Կարգավորվող պաշտպանության պրոֆիլներ * Ներկառուցված SD-WAN գործառույթ՝ առանց լրացուցիչ լիցենզավորման * Պետք է ունենա Trusted Platform Module (TPM) և Bluetooth Low Energy (BLE) տեխնոլոգիաների հնարավորություն   VPN պետք է ունենա տվյալ հնարավորությունները՝   * + PPTP, IPSec եւ SSL տեսակներ   + (DES, 3DES, AES) գաղտնագրում   + SHA-1/MD5, IKE-ի սերտիֆիկատի նույնականացում   + VPN PPTP, L2TP, IPSec NAT Traversal պրոտոկոլներ   + Հիերարխիկ (hub and spoke) VPN միացումներ   + Dead Peer Detection մեխանիզմ   Վեբ բովանդակության ֆիլտրման հնարավորությունները՝   * + URL/keyword արգելափակման հնարավորություն   + Whitelist URL ցուցակների գործածման հնարավորություն   + Аpplet Java, Cookies տարրերի արգելափակման հնարավորություն   + ActiveX-ի կառավարման հնարավորություն   + Վեբ-բովանդակության ֆիլտրման ծառայություններ, համացանցային ֆիլտր, firewall և proxy   Ներխուժման կանխարգելման համակարգ (IPS/IDS)՝   * + Դինամիկ բացահայտման սիգնատուրաների կարգվորվող ցանկ   + Հարձակման բազայի ավտոմատ թարմացման հնարավորթյուն   Սպամից պաշտպանվելու մոդուլի հնարավորություններ՝   * Blacklist ցուցակների իրական ժամանակի ռեժիմում «բաց վերահաղորդվող» տվյալների բազայի սերվերի հետ հաղորդակցվելու հնարավորություն * MIME վերնագրերի ստուգման հնարավորություն * Ֆիլտրում բանալի բառերով և արտահայտություններով * Blacklist-Whitelist IP հասցեների ցուցակների տեղադրման հնարավո-րություն * Իրական ժամանակում թարմացումները ավտոմատ ստանալու հնարավորություն   Պրոտոկոլի ձևակերպում/մոնիտորինգ՝   * + Լոգերի Syslog/WELF սերվերներին ուղարկելու հնարավորություն   + Իրական ժամանակում մոնիտորինգի եւ պատմությունների դիտման հնարավորություն   + Վիրուսների եւ հարձակումների մասին իրազեկման հնարավորություն էլեկտրոնային փոստով   + VPN թունելների մոնիտորինգ   + Cloud համակարգում լոգեր պահելու և մշակելու հնարավորություն   Պրոքսի-սերվեր՝   * Օգտատերերի կողմից հարցադրվող Web-կոնտենտի ֆիլտրացման հնարավորություն   Երաշխիք և ծառայությունների աջակցություն   * Սարքավորումները պետք է մատակարարվեն առնվազն 1 տարի երաշխիքային սպասարկմամբ: * Ներառված լինի 1 տարի ժամկետով Premium Support (24x7), UTP լիցենզիա 1 տարի ժամկետով * Հավելյալ՝ երկու սարք երկու արտոնագիր։ * Սարքերի տեղադրում կարգավորում։ * Երաշխիքի պայմանները պետք է ներառեն Web-պորտալի միջոցով արտադրողից տեխնիկական աջակցություն ստանալու հնարավորություն, առցանց չաթերի և հեռախոսի միջոցով տեխնիկական աջակցություն ստանալու հնարավորություն, սարքավորումների շարքից դուրս գալու դեպքում սարքավորումների փոխարինման հնարավորություն, համակարգի տեղադրված ծրագրային ապահովման տարբերակի թարմացում; * Մատակարար ընկերությունը սարքավորումների մատակարարման հետ մեկտեղ պետք է ներկայացնի MAF հավաստագիր։ | դրամ | Մ.Մկրտչյան 5 | 4-րդ եռամսյակ |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Услуга | | | | | |
| номер предусмотренного приглаше-нием лота | промежуточный код,  предусмотренный планом закупок по классификации  ЕЗК (CPV) | техническая характеристика | единица измере-ния | предоставление | |
| адрес | Срок |
| 1 | 64211340/6 | **Электронные информационные услуги, в том числе:**  высокопроизводительный межсетевой экран нового поколения с поддержкой UTM/UTP:  - Антивирус  - IPS/IDS  - Антиспам  - Фильтрация веб- и видеоданных  - Контроль приложений  - IP/домен ботнета  - Облачная песочница  Необходимо обеспечить возможность объединения устройств в кластер высокой доступности. Кластер должен работать в режиме «активный-активный», «активный-пассивный» или кластерном режиме.  Все устройства в кластере должны иметь централизованный интерфейс управления и мониторинга без необходимости использования дополнительных программных или аппаратных компонентов. Межсетевой экран должен обеспечивать следующие возможности:  – Межсетевой экран, IPsec, IPS, антивирус, антиспам, фильтрация контента, программное обеспечение для устройств, обнаружение вторжений, инструменты удаления рекламного и вредоносного ПО, расширенное обнаружение угроз, функции VPN, шейпинг трафика, функция точки доступа контроллера WLAN, проверка SSL в реальном времени (включая TLS 1.3), динамическая маршрутизация IPv4 и IPv6, оптимизация WAN-подключений, фильтрация веб- и видеоконтента, управление приложениями, интеграция с Active Directory, функция веб-прокси.  Межсетевой экран должен иметь как минимум:  – 18 аппаратно ускоренных портов GE RJ45, включая: 1 интерфейс GE RJ45 MGMT для управления, 1 интерфейс RJ45 HA и 16 портов коммутатора GE RJ45.  – 8 аппаратно ускоренных интерфейсов GE SFP.  – 4 аппаратно ускоренных интерфейса 10GE SFP+ (с поддержкой FortiLink).  – 1 консольный порт RJ45.  – 1 USB-интерфейс  - Все необходимые компоненты для установки в 19-дюймовую серверную стойку высотой не более 1 RU  - 2 блока питания (резервные блоки питания переменного тока, совместимые с PSU 80Plus для резервирования 1+1)  - Отдельный блок обработки безопасности (SPU)  Межсетевой экран должен обеспечивать следующие характеристики:  - Пропускная способность сети межсетевого экрана не менее 39 Гбит/с.  – Пропускная способность защиты от угроз: 2,8 Гбит/с  – Не менее 42 миллионов пакетов в секунду  – Пропускная способность IPSec VPN (512 байт): не менее 35 Гбит/с  – Пропускная способность SSL-VPN: не менее 1,5 Гбит/с  – Пропускная способность IPS: не менее 5,3 Гбит/с  – Количество одновременных сеансов (TCP): не менее 3 миллионов  – Количество новых сеансов: не менее 140 000 сеансов в секунду  – Количество одновременных подключений клиент-шлюз IPsec VPN: не менее 16 000  – Количество одновременных подключений шлюз-шлюз IPsec VPN: не менее 2000  – Количество политик межсетевого экрана: не менее 10 000  – Неограниченная пользовательская лицензия  – Блок обработки безопасности (SPU) должен обеспечивать пропускную способность 520 Гбит/с  Антивирусная защита от «сетевых червей» / Модуль обнаружения и уничтожения должен обладать следующими возможностями:  – Сканирование HTTP, SMTP, Протоколы POP3, IMAP, FTP и службы обмена мгновенными сообщениями, проверка зашифрованных VPN-туннелей  - Автоматическая доставка обновлений антивирусных баз «на лету»  - Возможность помещения зараженных сообщений в карантин  - Блокировка в зависимости от размера и типа файла  Сетевые функции:  - Поддержка SD-WAN, балансировка нагрузки, отказоустойчивость с возможностью использования нескольких WAN-интерфейсов  - Возможность работы в качестве PPPoE, DHCP, DNS-сервера  - Маршрутизация на основе политик, динамическая маршрутизация (RIP v1 и v2, OSPF, BGP, Multicast), возможность разделения зон, маршрутизация между зонами, маршрутизация между виртуальными сетями (VLAN)  - Возможность формирования логического интерфейса SD-WAN, объединяющего физические и логические интерфейсы с различными подключениями (MPLS, широкополосный интернет, LTE и т. д.)  - Оценка качества путей SD-WAN: пакетами или путем отправки запросов к определенным узлам сети  - Мониторинг характеристик путей в реальном времени (потеря пакетов, джиттер, задержка) и их графическое отображение  - Определение многоаспектных коммуникаций Стратегии выбора пути маршрутизации трафика приложений на основе критериев соответствия SLA, оптимальных значений характеристик коммуникационных путей и т. д.  - Маршрутизация трафика приложений и определение правил обслуживания по каналам SD-WAN с учетом стратегий и SLA  - Автоматическая балансировка нагрузки, коммутация и сохранение путей связи для используемых приложений и сервисов при изменении характеристик сетевых подключений (потери, джиттер, задержка) в режиме реального времени  - Динамическая коррекция потерь пакетов или восстановление ошибочных пакетов, вызванных неудовлетворительным состоянием WAN-путей при работе через VPN (ForwardError Correction)  - Балансировка пакетов в рамках одного сеанса через два VPN-туннеля IPSec на основе попакетной балансировки  Управление администрированием:  - Управление на основе ролей, несколько уровней администраторов и пользователей, обновления и изменения по протоколу TFTP и через веб-интерфейс, сохранение предыдущего состояния в системном программном обеспечении | драм | М.Мкртчяна 5 | 4-й квартал |